AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Northern District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Subject electronic devices currently secured at the Binghamton Resident Agency of the FBI, Binghamton, NY, more specifically described in Attachment A.

Case No. 3:20-MJ- 81 (ML)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Subject electronic devices currently secured at the Binghamton Resident Agency of the FBI, 15 Henry Stret, Suite 321, Binghamton, NY, more specifically described in Attachment A.

located in the Northern District of New York, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 2423(b)	Traveling in Interstate Commerce with Intent to Engage in Illicit Sexual Conduct
18 USC 2251(a)	Att. Sexual Exploitation for visual depiction/live visual
18 USC 2422(b)	Att. Coercion / Enticement

The application is based on these facts:

See Attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Jenelle C. Bringuel, SA, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 02/06/2020

Judge's signature

City and state: Binghamton, New York

Miroslav Lovric, United States Magistrate Judge

Printed name and title

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF NEW YORK

IN THE MATTER OF AN APPLICATION OF THE UNITED STATES OF AMERICA FOR SEARCH WARRANT FOR:

[SEE ATTACHMENTS A and B HEREIN]

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

JENELLE CORRINE BRINGUEL, being duly sworn, deposes and states:

INTRODUCTION

1. I am a Special Agent of the United States Department of Justice, Federal Bureau of Investigation ("FBI"), and I am empowered by law to investigate and make arrests for offenses enumerated in Title 18, United States Code, Section 2516. As such, I am an "investigative or law enforcement officer" within the meaning of Title 18, United States Code, Section 2510(7).

2. I have been employed as a Special Agent of the FBI since June 2012 and am currently assigned to the Albany Division, Binghamton Resident Agency. While employed by the FBI, I have investigated federal criminal violations related to cybercrime, child exploitation, and child pornography. I have gained experience through training by the FBI and everyday work relating to conducting these types of investigations. I have participated in the execution of several federal search warrants in child sexual exploitation investigations.

3. I am currently investigating Anthony Jacob Miceli and his traveling in interstate commerce with intent to engage in illicit sexual conduct, in violation of Title 18 United States Code, Section 2423(b), attempted sexual exploitation of children for the purpose of producing visual depictions of such conduct or for the purpose of transmitting a live visual depiction of such conduct, in violation of Title 18 United States Code, Section 2251(a), and using a facility and means of interstate and foreign

commerce to knowingly attempt to persuade, induce, entice, and coerce an individual who has not attained the age of 18 years to engage in any sexual activity for which any person can be charged with a criminal offense, in violation of Title 18, United States Code, Section 2422(b).

4. As will be demonstrated in this affidavit, there is probable cause to believe that evidence relating to violations of Title 18, United States Code, Sections 2423(b), 2251(a) and 2422(b) hereafter referred to as the "Subject Offenses" will be located on located on Miceli's: (A) Samsung Galaxy S10 cell phone, Model number SM-N975U, IMEI 359272100776360, and (B) Samsung Galaxy Note 8 with cracked back, hereafter, the "Subject Electronic Devices," as more fully described in Attachment A. The Subject Electronic Devices were retrieved from Miceli's person and vehicle during a probable cause arrest on February 3, 2020. I submit this affidavit in support of a search warrant authorizing a search of the Subject Electronic Devices as described in Attachment B, for evidence, fruits, and instrumentalities of the Subject Offenses. This affidavit and application are made under Fed. R. Crim. P. Rule 41 for authorization to search the Subject Electronic Devices.

5. The statements and facts set forth in this affidavit are based in significant part on: my review of electronic communications between Miceli and a law enforcement officer acting in an undercover capacity, and my personal training and experiences. Since this Affidavit is being submitted for the limited purposes of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts and circumstances that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violations of Title 18 United States Code, Sections 2423(b), 2251(a) and 2422(b) are presently located on the Subject Electronic Devices.

DEFINITIONS

6. The following definitions apply to this affidavit and Attachments A-B:

a. "Computer" refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and

includes any data storage facility or communications facility directly related to or operating in conjunction with such device." See 18 U.S.C. § 1030(e)(1).

b. "Computer-related documentation" consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

c. "Computer software" is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

d. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware.

e. "Computer passwords and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that

creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

f. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

g. "Minor" means any person under the age of 18 years. See 18 U.S.C. § 2256(1).

h. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); mechanical form (including, but not limited to, phonograph records, printing, typing); or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device.

BACKGROUND ON ELECTRONIC DEVICES AND CHILD EXPLOITATION

7. Based on my knowledge, training, and experience, and the experience and training of other law enforcement agents and investigators with whom I have had discussions, I know that electronic devices, including cellular telephones serve different roles or functions with respect to child exploitation.

8. As with most digital technology, communications made from a cellular telephone are often saved or stored on that device's hard drive or memory card. Storing this information can be intentional, for example, by saving an e-mail as a file, or saving the location of a favorite website in "bookmarked" files. Digital information, however, can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, users' Internet activities generally leave traces that a trained digital forensic examiner often can recover, including evidence and other items that show whether a cellular telephone was sharing data files, and some of the data files that were uploaded, downloaded and transferred. Such information is often maintained indefinitely until overwritten by other data.

9. Modern technology in the past several years has transformed the cellular telephone from a simple mobile telephone device into a mobile mini-computer commonly referred to as a "smart phone" capable of Internet access through wireless internet connections as well as cellular telephone signals; built in digital camera and video camera capabilities are common features; video and image storage capabilities can hold thousands of images and hours of video files; and by being able to access the Internet virtually anywhere, digital images and videos taken with a cellular telephone and stored on the cellular telephone can be shared with others by e-mail (phone to computer), text messaging (phone to phone), and uploaded to and displayed on Internet websites. Smart phones generally have global positioning satellite (GPS) capabilities that allow the cellular telephone to provide driving directions, and include GPS coordinates in such features as sharing locations on social networking websites and imbedding into the metadata of photographic images the coordinates of where an image was taken.

INDIVIDUALS INTERESTED IN CHILD EXPLOITATION

10. Individuals who seek out sexual activity with minors may search for and seek out other

like-minded individuals or minors, either in person or on the Internet, as a means of seeking other victims. This contact also may help these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to: text messages, video messages, electronic mail, email, bulletin boards, IRC, chat rooms, newsgroups, instant messaging, and other vehicles.

11. Individuals who seek out sexual activity with minors may maintain stories, books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children, as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals may keep these materials because of the psychological support they provide.

12. Individuals who seek out sexual activity with minors may keep names, electronic mail addresses, cellular and telephone numbers, or lists of persons who have shared, advertised, or otherwise made known their interest in sexual activity with minor children. These contacts may be maintained as a means of personal referral, exchange, and/or commercial profit. This information may be maintained in the original medium from which it was derived.

BACKGROUND OF THE INVESTIGATION

13. On or about January 8, 2020, a law enforcement officer acting in an undercover capacity (the "UC") posted a description in the "about me" section on a social-networking and dating application located on the internet. The description used language that is commonly associated with individuals seeking children for sexual purposes.

14. On or about January 25, 2020, the UC received a message on the geo-location based social-networking application that read, "Hii." On that same date, the UC replied to the message by typing, "Hey." A few minutes later, the UC received another message asking, "What's uppp?," and then "What you looking for??" and then, "On here." The messages were from a person with the username "AJ." The geo-location of the user was Tobyhanna, Pennsylvania. The UC replied to the messages by typing: "You read my profile."

15. The UC and user "AJ" (later identified as Anthony Jacob Miceli) began exchanging messages. Miceli indicated he was into "yng" which commonly indicates the individual is attracted to or interested in engaging in sexual acts with young individuals and/or children. The UC posed as a parent with two young daughters, ages eight and five. Miceli expressed an interest in meeting up to engage in sexual acts with the UC's daughters.

16. During the course of ensuing text message conversations and phone conversations, which occurred from January 25, 2020 to February 3, 2020, the UC and Miceli discussed Miceli's desire to travel from Pennsylvania to engage in sexual acts with the UC's daughters in Broome County, New York. Consistent with the geo-location from the social-networking application, Miceli told the UC that he lived in Tobyhanna, Pennsylvania and "would like to meet asap."

17. Miceli proposed various scenarios to engage in sexual acts with the UC's daughters once he traveled to UC's residence in Broome County, including that the UC could leave UC's daughters with him and he would live-stream the sexual contact with the children to the UC. In later conversations, the UC asked Miceli how live-streaming worked and whether Miceli would record the live-stream of UC's children. Miceli told UC that recording a live-stream is "just super incriminating; my safety is my number one concern." He continued by saying "[t]his is a serious thing..."

18. The UC asked Miceli "[i]f im not gona be there though...can we talk about what you would do with each of them?" Miceli was initially resistant to discussing via message what sexual acts he intended to perform on the children, however, later asked the UC "[i]f I got a test for you this week could I skip on the rubber[?]" The UC understood the defendant to be asking whether, if the defendant took a test to confirm that he did not have sexually transmitted diseases, he could have intercourse with the children without using a condom. Later in the communication, Miceli asked the UC whether UC's daughters had ever "played with a cock before." When UC responded in the negative, Miceli stated "Cannot wait to introduce them...". He continued by stating "I'll have to wear some sweatpants ;) haha" and "Mmm I want them to play with my cum."

19. On January 29, 2020, Miceli asked the UC to switch to a different social-networking application where he and the UC could talk "privately." During the initial conversation between the UC and Miceli on the new social-networking application, Miceli told the UC "...now we can talk about whatever and not have to worry because I was being extremely hesitant. Now you got my trust 100%." Shortly thereafter, Miceli told the UC that Miceli "...got that young pussy in the back of my mind... I cannot wait to taste it. Very Excited to see the look on their faces when they see my big cock in front of them.... Mmm and those tiny hands grabbing on it." Miceli said that he planned to "...get in [the children's] pants also and start rubbing on and eating them out, show them they can put me in their mouths too."

20. During the course of the messages, the UC and Miceli agreed that Miceli would travel to meet UC and the UC's children in Broome County on Monday, February 3, 2020. The UC suggested that Miceli could bring a small gift or toy for the UC's children in order to "break the ice," and suggested items involving "puppies" or unicorns. On January 31, 2020, Miceli told the UC that he also planned to bring a vibrator to use on one of the UC's children. Miceli stated "I think this vibrator will help me out. It kinda looks like a toy so we can play around and be silly with it then I'll stick it between her legs and ask how it feels haha I'll send you a pic of it." Miceli follow up by sending UC a photograph of a vibrator. Miceli also sent the UC various pictures and videos of Miceli's body parts, including Miceli masturbating. Further, Miceli sent identifying pictures of himself and a relative.

21. The acts described in the messages with the UC, if committed, would violate the following sections of the New York State Penal Law, among others: Rape in the First Degree in violation of Penal Law Section 130.35(3); Criminal Sexual Act in the First Degree in violation of Penal Law Section 130.50(3); and Sexual Abuse in the First Degree in violation of Penal Law Section 130.65(3).

22. On February 3, 2020, Miceli arrived at a residence in Broome County, in the Northern District of New York, where, as described above, he had made arrangements to meet the UC, the eight year old child and the five year old child. Upon Miceli's arrival at the residence, he and the UC, who was still in role as the parent, engaged in conversation. Miceli appeared to be the same person depicted in

some of the photographs sent to the UC. Further, Miceli sounded like the same person that the UC had previously spoken to via telephone. Further, in the in person recorded conversation between the UC and Miceli on February 3, 2020, the exchange was a continuation of the dialogue that the UC had been engaging in with user AJ from January 25, 2020, on both social-networking applications and over the phone. Throughout the course of messages and the recorded conversation between the UC and Miceli, Miceli told the UC that he had driven directly from his work to Broome County to engage in sexual acts with the UC's daughters, and that he purchased lubricant at a pharmacy on the way to the UC's residence. Miceli also told the UC that he brought the vibrator and other sex toy, depicted in his prior messages to the UC, to use in sexual acts involving UC's children. Miceli further stated that he brought a tripod in order to set up his phone to live-stream himself engaged in sex acts with the UC's daughters.

23. Following these statements to the UC, Miceli was placed under arrest. The Samsung Galaxy Note 8 phone was recovered in the defendant's vehicle. The Samsung Galaxy S10 phone was on the defendant's person. The defendant was carrying a backpack which contained a vibrator, silicone sex toy, tripod and lubricant. Upon a search of his vehicle, police located an identification and other identifying information, a passport and another container of lubricant. The defendant was given his *Miranda* Warnings, and agreed to speak to police and allow them to search of his phones. Miceli provided the passcode pattern for his Galaxy S10 phone. Miceli told law enforcement that he deleted all the chats and the social-networking applications he had communicated on with the UC prior to arriving at the residence in Broome County. Miceli also admitted that he traveled from work in Hawley, Pennsylvania. Miceli later withdrew consent to search his phones.

24. Your affiant is aware the social-networking applications that Miceli was communicating with the UC on are most frequently located on cellular phones. Further, your affiant is aware that the UC continued to communicate with Miceli via social-networking application until Miceli arrived in Broome County to meet with the UC and her children. Specifically, Miceli messaged with the UC as he was driving to Broome County, sent pictures of his vehicle and scenery as he was traveling, and messaged the UC when he had arrived. Accordingly, there is probable cause to believe that evidence of the Subject

Offenses, including Miceli's conversations with the UC, the photographs of the vibrator sent to the UC, and other photographs exchanged during the course of the communication between Miceli and the UC, will be located on the Subject Electronic Devices.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

25. Your Affiant is trained in electronic evidence recovery and, further, has spoken with law enforcement investigators trained in computer and cellular telephone evidence recovery that have extensive knowledge about the operation of cellular telephones and computer systems including the correct procedures for the seizure and analysis of these systems.

26. Based on my knowledge, training, and experience, your Affiant is aware that electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, transferred, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost to the user. Even when files have been deleted, they can be recovered months or years later using specialized forensic tools. This is so because when a person "deletes" a file on a computer or cellular telephone, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

27. Therefore, deleted files or remnants of deleted files may reside in free space or slack space—that is, in space located on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data or process in a "swap" or "recovery" file.

28. Apart from user-generated files, an electronic device may contain electronic evidence of it was used, what it was used for, and more importantly, who used it recently and in the past. This evidence can take the form of operating system configurations, artifacts from operating system or different application operation, file system data structures, and the virtual memory "swap" or paging files. Similarly, files viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache" located on the computer. The browser often maintains a fixed amount of hard drive

space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

29. Although some of the information called for by this search warrant might be found in the form of user-generated documents (such as photographic images and video files), smart phone style cellular telephones can contain other forms of electronic evidence as well:

a. Forensic evidence of how the Subject Electronic Devices were used, the purpose of its use, who used it, and when, is called for under this request for a search warrant. Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Computer file systems can record information about the dates and times files were created and the sequence in which they were created.

b. Forensic evidence on an electronic device can also indicate who has used or controlled it. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence or physical location. For example, registry information, configuration files, user profiles, e-mail address books, "chats," instant messaging logs, photographs, and correspondence (and the data associated with the foregoing, such as file creation and last accessed dates and times) may in and of themselves be evidence of who used or controlled the computer or storage medium at a relevant time in question.

c. A person with appropriate familiarity with how an electronic device works can, after examining this forensic evidence in its proper context, draw logical conclusions about how it was used, the purpose of its use, who used it, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance with particularity a description of the records to be sought, evidence of this type often is not always data that can be merely reviewed by a review team and passed along to the case agents and investigators. Whether data stored on an electronic device is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand the nature of the evidence described in Attachment B also falls within the scope of the search warrant.

e. Searching storage media for the evidence described in the Attachment B may require a range of data analysis techniques. It is possible that the storage media will contain files and information that are not called for by the search warrant. In rare cases, when circumstances permit, it is possible to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. For example, it is possible, though rare, for a storage medium to be organized in a way where the location of all things called for by the search warrant is immediately apparent. In most cases, however, such techniques may not yield the evidence described in the search warrant. For example, information regarding user attribution or Internet use is located in various operating system log files that are not easily located or reviewed. As explained above, because the search warrant calls for records of how the Subject Electronic Device was used, what it was used for, and who used it, it is likely that it will be necessary to thoroughly search the device to obtain evidence including evidence that is not

neatly organized into files or documents. Just as a search of a premises for physical objects requires searching the entire premises for those objects that are described by a search warrant, a search the Subject Electronic Devices for the things described in this search warrant will likely require a search among the data stored in storage media for the things (including electronic data) called for by this search warrant. Additionally, it is possible that files have been deleted or edited, but that remnants of older versions are in unallocated space or slack space. This, too, makes it exceedingly likely that in this case it will be necessary to use more thorough techniques.

SEARCH METHODOLOGY TO BE EMPLOYED: THE SUBJECT ELECTRONIC DEVICES

30. The search procedure of electronic and digital data contained in cellular telephones, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. examination of all of the data contained in such cellular telephone and its memory storage device to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying various file directories and the individual files they contain;

d. opening files in order to determine their contents and scanning storage areas;

e. performing key word searches to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and

f. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

BIOMETRIC UNLOCKING TECHNOLOGY

31. As described above, two cellular devices were secured from the defendant at the time of his arrest.

32. The Samsung Note 8 phone was unlocked when it was secured by law enforcement. Law enforcement does not know a passcode or password for this device. While the device appears to continue to be unlocked, if this phone were to lock, it would likely be necessary to use biometric features of the user of the cell phone in an attempt to unlock the device for the purpose of executing the search authorized by this warrant.

33. The Samsung S10 phone is locked. However, before he revoked consent to search, Miceli gave law enforcement the pattern code to unlock the phone. However, if this code does not work, it may become necessary to use biometrics of the user of the cell phone in an attempt to unlock the device for the purpose of executing the search authorized by this warrant.

34. I know from my training and experience, as well as from information found in publicly available materials including those published by Samsung, that some models of Samsung devices offer their users the ability to unlock the device via biometric features in lieu of a numeric or alphanumeric passcode or password.

a. The biometric features available on the Samsung Galaxy Note 8 Phone include fingerprint and iris recognition. The user of the Subject Device can select which biometric feature or combination of features to utilize.

b. The biometric features available on the Samsung Galaxy S10 Phone include fingerprint and facial recognition. The user of the Subject Device can select which biometric feature or combination of features to utilize.

35. On fingerprint unlock enabled devices, a user can register multiple fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's sensor.

36. If the facial recognition feature is enabled, a user can register his or her face to be used to unlock the Subject Electronic Device. To activate the facial recognition feature, a user must hold the Subject Electronic Device in front of his or her face. The Subject Electronic Device's front-facing camera next analyzes and records data based on the user's facial characteristics. The Subject Electronic Device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face.

37. If an iris recognition feature is enabled, a user can register one or both of his or her irises to be used to unlock the Subject Electronic Device. To activate the iris recognition feature, the user holds the device in front of his or her face. The Subject Electronic Device next directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises.

38. In my training and experience, users of electronic devices often enable the biometric features (as described above) because they are considered to be a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to

protect the device's contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

39. Finally, your Affiant is aware that Samsung devices allow specific folders to be protected by biometric technology, i.e. biometrics may be required to access specific folders. Specifically, your Affiant is aware that biometrics may be necessary to disable a locking feature which would prevent the examiner from accessing a setting necessary to execute the search of the Subject Electronic Devices. Thus, law enforcement personnel may not otherwise be able to access the data contained within the Subject Electronic Devices, making the use of the devices' biometric features necessary to the execution of the search authorized by this warrant.

40. These devices were found on the person or in the car of the defendant and the defendant admitted that the devices were his. Based on these facts and my training and experience, it is likely that the defendant, Anthony Miceli, is the user of the Subject Electronic Devices and thus that fingerprint, face, or irises are among those that are able to unlock the Subject Electronic Devices via biometric features.

41. Due to the foregoing, I respectfully request that the Court authorize law enforcement to press or swipe the fingers (including thumbs) of Anthony Miceli to the Subject Electronic Devices' fingerprint scanners, hold the Subject Electronic Devices in front of Anthony Miceli's face and activate the facial recognition feature and/or hold the Subject Electronic Device in front of Anthony Miceli's face and activate the iris recognition feature, if necessary, for the purpose of attempting to unlock the Subject Electronic Devices in order to search the contents as authorized by this warrant.

CONCLUSION

42. Based upon the above information, there is probable cause to believe that evidence of violation of Title 18, United States Code, Sections 2423(b) (traveling in interstate commerce with intent to engage in illicit sexual conduct), 2251(a) (attempted sexual exploitation of a minor for the purpose of

producing visual depictions of such conduct or for the purpose of transmitting a live visual depiction of such conduct), and 2422(b) (attempted coercion and enticement of a minor) as outlined in Attachment B of this Affidavit, will be found on the Subject Electronic Devices that are the subject of this warrant as set forth in Attachment A. Therefore, based upon the information contained in this affidavit, your Affiant requests this Court issue the attached search warrant authorizing the search of the contents of the Subject Electronic Devices set forth in Attachment A for the items more particularly described in Attachment B.

Jenelle Corrine Bringuel
Special Agent
Federal Bureau of Investigation

Sworn to before me this 6th day
of February 2019.

HONORABLE MIROSLAV LOVRIC
UNITED STATES MAGISTRATE JUDGE
NORTHERN DISTRICT OF NEW YORK

ATTACHMENT A

DESCRIPTION OF THE SUBJECT ELECTRONIC DEVICE TO BE SEARCHED

The Subject Electronic Devices are currently secured at the FBI Binghamton Resident Agency, 15 Henry Street, #321, Binghamton, NY 13901, and are fully identified and described below as follows:

The Subject Electronic Devices:

- Samsung Galaxy S10 cell phone, Model number SM-N975U, IMEI 359272100776360
- Samsung Galaxy Note 8 with cracked back

ATTACHMENT B

ITEMS AND INFORMATION TO BE SEARCHED FOR AND SEIZED

Items and information that constitute fruits, evidence and instrumentalities of violations of Title 18, United States Code, Sections 2251(a) (attempted sexual exploitation of children for the purpose of producing visual depictions of such conduct or for the purpose of transmitting a live visual depiction of such conduct), 2423(b) (traveling in interstate commerce with intent to engage in illicit sexual conduct), and 2422(b) (attempted coercion and enticement of a minor to engage in any sexual activity for which any person can be charged with a criminal offense.)

1) Correspondence, text messages, chats, and other communications demonstrating an intent, and/or attempt to (a) use a person under the age of eighteen to engage in sexually explicit conduct for the purpose of live-streaming or producing visual depictions of such conduct, (b) travel in interstate commerce for the purpose of engaging in illicit sexual conduct, or (c) coerce or entice a minor to engage in any sexual conduct for which any person could be charged with a crime, whether directly or through an intermediary, and communications that show planning to engage in any such conduct.

2) Images sent or received in connection with the commission or attempted commission of the above offenses, including images of the defendant, his relative, the UC, sexual toys, maps and scenery and vehicle images sent while defendant was traveling to meet UC.

3) Any and all documents and records pertaining to any plan to carry out the listed offenses, including maps, directions, internet history, or other evidence of plans to travel in interstate commerce for the purpose of engaging in unlawful sexual conduct, and/or to live-stream or otherwise produce images depicting children engaged in sexually explicit conduct.

4) Data showing the use or ownership of the subject electronic devices, and any Internet accounts accessed through the devices, including evidence of Internet user names, screen names or other Internet user identification.

5) Passwords and data security devices, meaning any devices, programs, or data that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any electronic hardware, software, documentation, or electronic data records.

6) Records or identifying information for ANTHONY MICELI and evidence of his ownership and/or possession of the media being analyzed.

7) Evidence of Snapchat user Xsr450, Skout user A.J., and text message communication utilizing (570) 982-9150.

Biometric Unlock

During the execution of the search of the Subject Electronic Devices described in Attachment A, law enforcement personnel are authorized to press or swipe the fingers (including thumbs) of Anthony Miceli to the Subject Electronic Devices' fingerprint scanners, hold the Subject Electronic Devices in front of Anthony Miceli's face and activate the facial recognition feature and/or hold the Subject Electronic Devices in front of Anthony Miceli's face and activate the iris recognition feature for the purpose of attempting to unlock the Subject Electronic Devices in order to search the contents as authorized by this warrant.